Figure 1

Web Client 100

Internet 50

SSL session with encrypted traffic between Client and SSL Accelerator

Router 75

SSL Accelerator 250

HTTP session with clear text traffic between SSL Accelerator and Web Servers

Web Servers 300

Figure 2A

100

250

300

Web client ← SSL/HTTPS/TCP → SSL Accelerator ← HTTP/TCP → Web server

HTTP		HTTP		HTTP		HTTP
SSL		SSL				
TCP		TCP		TCP		TCP
IP	HTTPS/443	IP		IP	HTTP/80	IP

Web client

SSL accelarator

Web server

Figure 2B

FIGURE 4

Client 100	Server 300
	Listen
Syn	→ Syn_Received
Active Open/Syn_sent ←	ACK+SYN
Established /ACK	→ (ACK Received) Link Established.

HTTP				HTTP
SSL				TCP
TCP	HTTPS/443	IP SSL IP	HTTP/80	IP
IP				

Web client   SSL accelarator   Web server

FIGURE 3

FIGURE 5 (Direct Mode)

Client 100 1.1.1.1	SSL AD 250 2.2.2.2	SERVER 300 3.3.3.3

Send SYN to 3.3.3.3 202 — Port 443 →

Intercept Packet Destined for Server 300; Reduce MSS to Accommodate Headers And Extensions if necessary; Forward On to server. (204) — Port 80 →

Receive SYN Packet 206

Send ACK to Client at 1.1.1.1 Using server 300 IP as source IP 210 — Port 80 ←

Send TCP SYN, ACK to Client 1.1.1.1 208

Forwards ACK 214

Receive Client ACK

Send ACK to 3.3.3.3 212

Start SSL Handshake with Server 300 (220)

SSLAD sends appropriate responses to client using server 300's IP using server's IP 3.3.3.3 (230)

Handshake Negotiation (235)

Send Encrypted Application Data (265)

Decrypt Packet, SSL Record; Save TCP Sequential Number, SSL Sequential Number, Initialization Vector (IV), & Expected ACK (for DES) in SSL TCP database; FORWARD PACKET IN CLEAR TO PORT 80 (270)

Receive clear Packet on Port 80, process and return 275

Receive and Decrypt Server Packet (282)

Receive Clear Packet. Extract ACK, compare with all expected Server ACKs and clear all entries which have expected ACK's less than or equal to received ACK; Save TCP Sequential Number and SSL Sequential Pair in SSL TCP database; Encrypt & Forward Packet (280)

Send ACK (284)

Receive Client ACK

Receive ACK, compare with all expected Client's ACKs and clear all entries which have expected ACK's less than or equal to received ACK; Forward ACK (285)

(continue for session duration)

RESET

Clear database on kill connection

FIGURE 6 (Load Balance Mode)

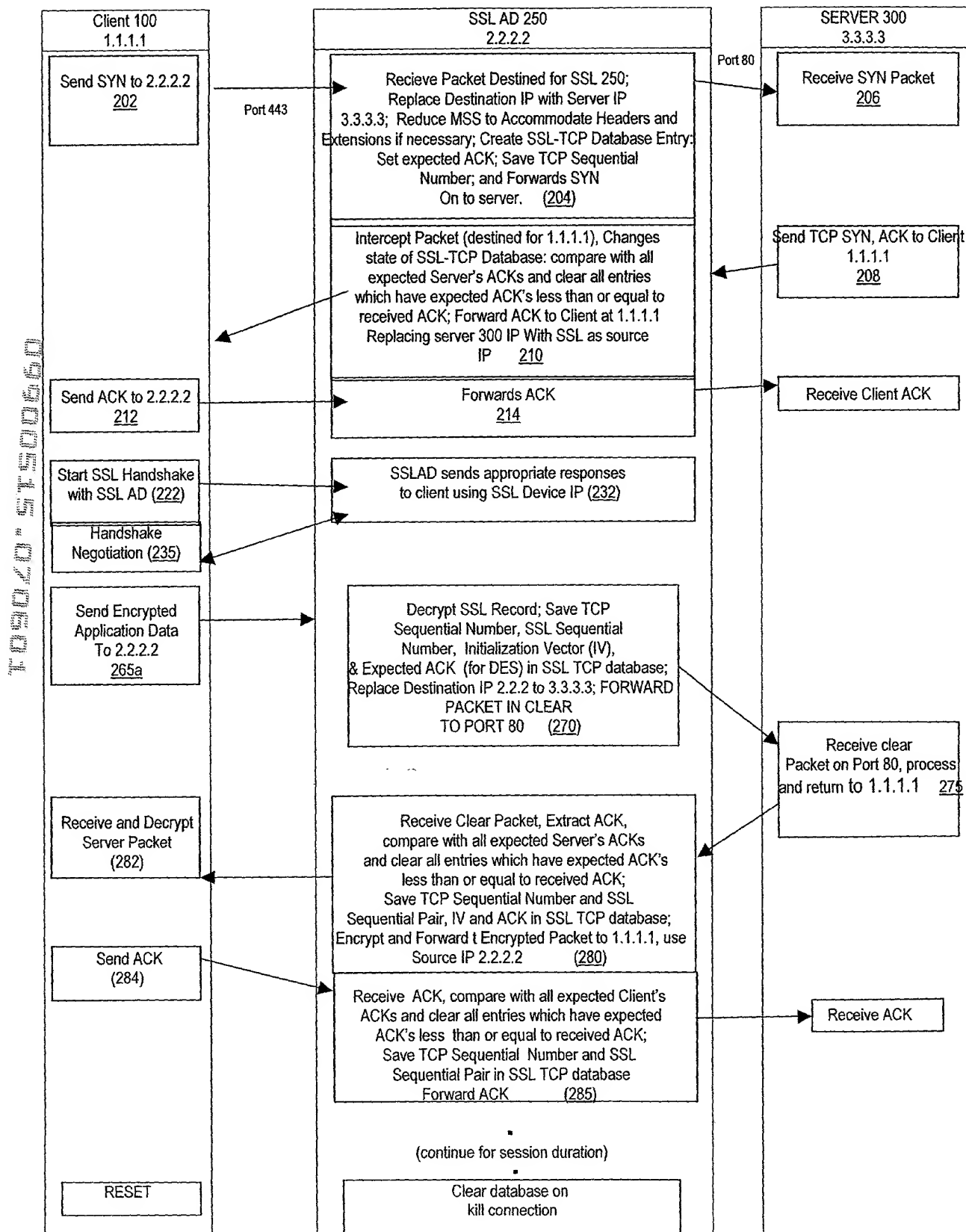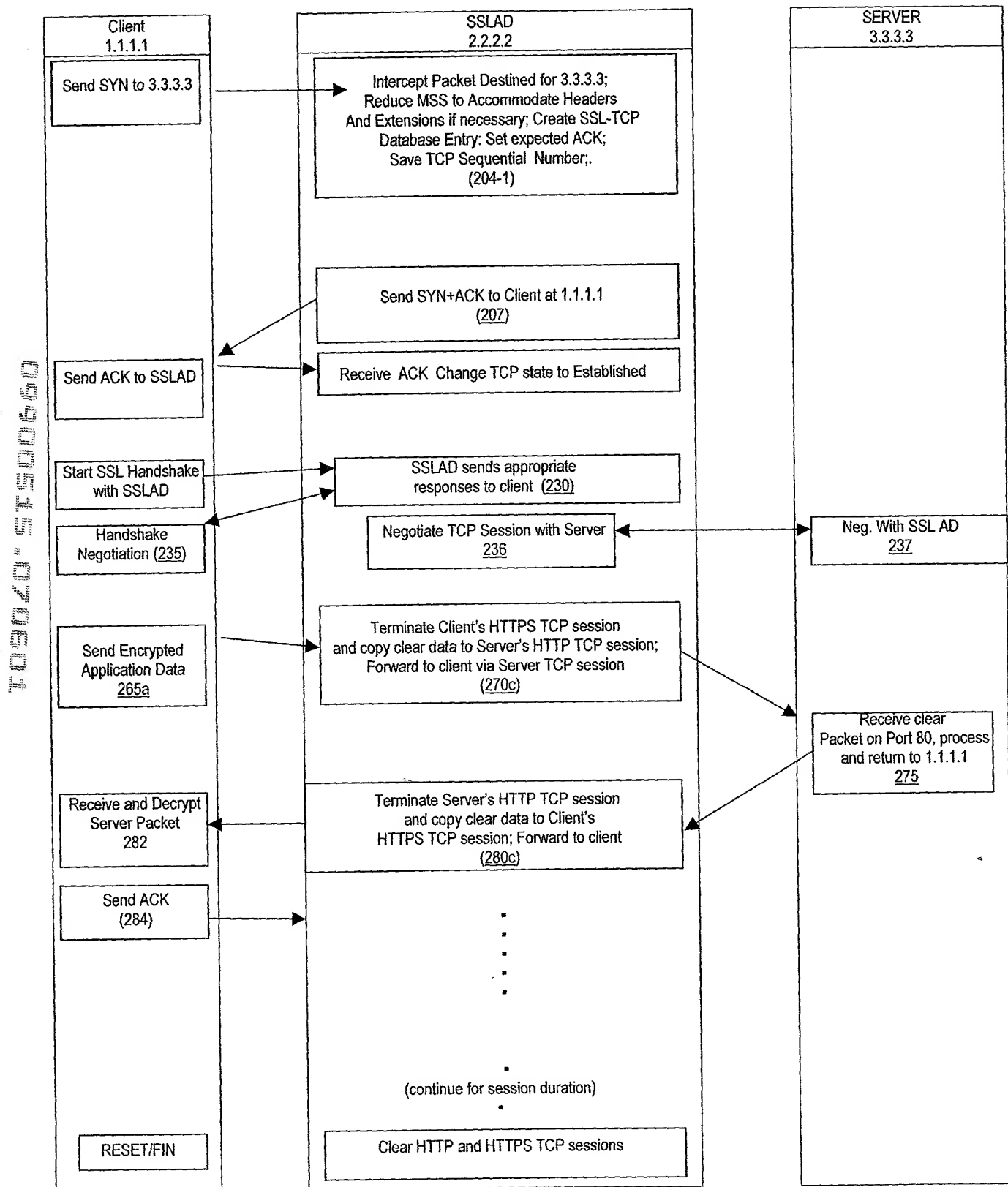| Client 100 1.1.1.1	SSL AD 250 2.2.2.2	SERVER 300 3.3.3.3
Send SYN to 2.2.2.2 **202**	Recieve Packet Destined for SSL 250; Replace Destination IP with Server IP 3.3.3.3; Reduce MSS to Accommodate Headers and Extensions if necessary; Create SSL-TCP Database Entry; Set expected ACK; Save TCP Sequential Number; and Forwards SYN On to server. **(204)**	Receive SYN Packet **206**
	Intercept Packet (destined for 1.1.1.1), Changes state of SSL-TCP Database: compare with all expected Server's ACKs and clear all entries which have expected ACK's less than or equal to received ACK; Forward ACK to Client at 1.1.1.1 Replacing server 300 IP With SSL as source IP **210**	Send TCP SYN, ACK to Client 1.1.1.1 **208**
Send ACK to 2.2.2.2 **212**	Forwards ACK **214**	Receive Client ACK
Start SSL Handshake with SSL AD **(222)**	SSLAD sends appropriate responses to client using SSL Device IP **(232)**	
Handshake Negotiation **(235)**		
Send Encrypted Application Data To 2.2.2.2 **265a**	Decrypt SSL Record; Save TCP Sequential Number, SSL Sequential Number, Initialization Vector (IV), & Expected ACK (for DES) in SSL TCP database; Replace Destination IP 2.2.2 to 3.3.3.3; FORWARD PACKET IN CLEAR TO PORT 80 **(270)**	Receive clear Packet on Port 80, process and return to 1.1.1.1 **275**
Receive and Decrypt Server Packet **(282)**	Receive Clear Packet, Extract ACK, compare with all expected Server's ACKs and clear all entries which have expected ACK's less than or equal to received ACK; Save TCP Sequential Number and SSL Sequential Pair, IV and ACK in SSL TCP database; Encrypt and Forward t Encrypted Packet to 1.1.1.1, use Source IP 2.2.2.2 **(280)**	
Send ACK **(284)**	Receive ACK, compare with all expected Client's ACKs and clear all entries which have expected ACK's less than or equal to received ACK; Save TCP Sequential Number and SSL Sequential Pair in SSL TCP database Forward ACK **(285)**	Receive ACK
	(continue for session duration)	
RESET	Clear database on kill connection	

Port 443

Port 80

FIGURE 7 (Full TCP Proxy Mode)

Figure 8

Normal SSL Record

IP/TCP Header	SSL Header	DATA	HMAC MD5 SHA, etc.	Pad/Pad Length

Multi-Segment:

IP/TCP Header	SSL Header	Data

IP/TCP Header	DAT A		HMAC MD5 SHA, etc.	Pad/Pad Length

Figure 9a

Figure 9b